B. Remarks

Claims 1-20 are pending in the application. The examiner previously rejected claims 1, 5, 11, and 15 under 35 U.S.C. § 102(b) as being anticipated by Ganesan, U.S. Patent No. 5,557,678 and claims 2-4, 6-8, 12-14, and 16-18 under 35 U.S.C. § 103(a) as being unpatentable over Ganesan in view of Patel, U.S. Publication No. 2002/0071558 A1. Applicants previously responded, arguing that Ganesan does not teach or suggest the unique combination of steps recited in these claims. The examiner was not persuaded by Applicants' arguments and has now made final her rejection of these claims. Applicants maintain their position that the present invention is fundamentally different from Ganesan and that Ganesan does not teach or suggest the unique combination of steps recited in these claims. As such, Applicants respectfully request reconsideration.

Applicants' present invention is directed to a method for securely providing encryption keys for encrypting and decrypting data. According to the present invention, an initial software product for use on a hardware product is encrypted using a first encryption key. This same first encryption key is split into first and second key portions. The first and second key portions and the encrypted initial software product are provided for use in a hardware product. The first and second key portions are combined to yield the first encryption key, which is used to decrypt the initial software product. As such, the same encryption key is used both to encrypt and decrypt the data. These limitations are articulated in claim 1 (and, therefore, in each of its dependent claims 2-10), which recites:

> A method for enabling encryption and decryption of an initial version of a software product comprising the steps of:
>
> generating a first encryption key;

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;

generating a first key portion of said first encryption key;

calculating a second key portion by utilizing said first key portion and said first encryption key to generate a said second key portion such that the combination of said first key portion and second key portion form said first encryption key;

providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product;

combining said first key portion and said second key portion to provide said first encryption key in said hardware product; and

utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product.

The examiner contends that Ganesan discloses the foregoing combination of steps. Specifically, the examiner has stated that Ganesan teaches "generating a first encryption key (Ganesan Fig. 2 No. 202); [and] encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (Ganesan Fig. 2 No. 220; encrypting the message (software product) with the first key)." Office Action at 4. Applicants respectfully submit that this characterization of Ganesan is incorrect. Indeed, Ganesan teaches that "in step 202 the private encryption keys and public encryption keys are generated by central security processor 50 for each user of the system." Ganesan at col. 8, ll. 26-28. Ganesan further teaches that "in step 218 a message is generated on Station 30. The message is encrypted in step 220 by the station 30 processor with the session key." Ganesan at col. 9, ll. 19-21. Importantly, however, the session key Ganesan uses to encrypt the message in step 220 is <u>not</u> one of the keys generated in step 202. Indeed, the keys generated in step 202 and the key used to encrypt the message in step 220 are <u>different keys.</u> For this reason alone, Ganesan does not anticipate Applicants' claims.

The examiner further contends that Ganesan discloses "generating a first key portion of said first encryption key (Ganesan Fig. 2 No. 202, and col. 2 lines 52-58; d.sub.i); calculating a second key portion . . . combining said first key portion and said second key portion to provide said first encryption key in said hardware product (Ganesan Col. 2 lines 56-59; d=di*dj); and utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product (Ganesan Col. 2 lines 56-59, col. 6 lines 1-19, and Fig. 2 No. 222; decrypting the message (software product) using the key (the first and second key portion of the key is the first encryption key))." Office Action at 5. Applicants respectfully submit that this characterization of Ganesan also is incorrect. To the extent that Ganesan discloses splitting keys into key portions, for example, at step 204, Ganesan does not disclose recombining these key portions to yield an original key and using this recombined, orignal key to decrypt an initial software product, message, or data.

Based on at least the above arguments, Applicants respectfully submit that claim 1 and claims 2-10 that depend from claim 1 distinguish over and are allowable over the cited references. Also, Applicants respectfully submit that claims 11-20 distinguish over and are allowable over the cited references for similar reasons. Further, Applicants respectfully submit that the examiner's rejections of dependent claims 2-4, 6-8, 12-14, and 16-18 under 35 U.S.C. § 103(a) are moot in view of the above. As such, Applicants respectfully submit that the pending claims are allowable over the cited references and respectfully request reconsideration toward that end.

Applicants respectfully request entry of the previously submitted and presently re-submitted amendment to the specification to include the government interest statement required by 35 U.S.C. § 202(c)(6).

Respectfully submitted,

Date: September 7, 2005

Mark P. Vrla
Registration No. 43,973
Attorney for Applicant

JENNER & BLOCK LLP
One IBM Plaza
Chicago, IL 60611
Ph. (312) 222-9350
Fax (312) 840-7657